

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

---

<p><b>RISHAV SHARMA</b>, individually and on behalf of all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p><b>MKS INSTRUMENTS, INC.</b>,</p> <p style="text-align: center;">Defendant.</p>	<p>Case No. 1:23-cv-10948</p> <p style="text-align: center;"><b>JURY TRIAL DEMANDED</b></p>
--	---

---

**FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiff, Rishav Sharma, individually and on behalf of the Class defined below of similarly situated persons, alleges the following against MKS Instruments, Inc. (“MKS” or “Defendant”) based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff’s counsel and review of public documents as to all other matters:

**INTRODUCTION**

1. Plaintiff brings this class action against MKS for its failure to properly secure and safeguard Plaintiff’s and other similarly situated current and former employees’ (“Class Members”) personally identifying information from hackers. According to the company, this information can include names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs (where MKS is required by law to collect), education, employment history, dates of birth, gender, sexual orientation, bank account information, payment card information, information about compensation and equity, information

about job position and time/hours worked, information about disabilities, health and medical conditions, employer union, health insurance information, basic information regarding partners, children and emergency contacts (such as name, age, and contact details), if applicable<sup>1</sup> (the “Private Information”).

2. On February 3, 2023, MKS, a semiconductor equipment maker, suffered a ransomware attack that required it to suspend operations at some of its facilities, and which resulted in the compromise and exfiltration of Plaintiff’s and Class Members’ Private Information (the “Data Breach”). Through the Data Breach, the cybercriminals were able to access files containing current and former employees’ Private Information and, according to the data breach notice sent to Plaintiff and Class Members, the Data Breach “may have also involved *exfiltration* of personal data” (emphasis added).

3. As a result of the Data Breach, Plaintiff and Class Members are at a substantial and imminent risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

4. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, government ID numbers (including Social Security numbers), financial information, and protected health information (“PHI”) that MKS collected from its current and former employees and maintained in its system.

5. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members’ names, taking out loans in Class Members’ names, using Class Members’ information to obtain

---

<sup>1</sup> See <https://www.databreaches.net/mks-instruments-breach-notification-includes-a-surprising-statement-to-reassure-those-affected/> (last visited on April 27, 2023).

government benefits, using Class Members' information to obtain medical treatment and/or prescription drugs in their name, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

6. There has been no assurance offered by MKS that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

7. Therefore, Plaintiff and Class Members are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

8. Plaintiff brings this class action lawsuit to address MKS's inadequate safeguarding of his and Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access *and exfiltration* by cybercriminals.

9. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to MKS, and thus MKS was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

10. Plaintiff's and Class Members' identities are now at risk because of MKS's negligent conduct as the Private Information that MKS collected and maintained is now in the hands of data thieves and other unauthorized third parties.

11. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

12. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, and declaratory and injunctive relief.

### I. PARTIES

13. Plaintiff Rishav Sharma is an individual citizen of the State of Utah.

14. Defendant MKS, Inc. is headquartered at 2 Tech Drive, Ste. 201, Andover, MA 01810.

### II. JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from MKS. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

16. This Court has jurisdiction over MKS because MKS operates in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because a substantial part of the events giving rise to this action occurred in this District and MKS has harmed Class Members residing in this District.

### III. FACTUAL ALLEGATIONS

#### A. *MKS's Business and Collection of Plaintiff's and Class Members' Private Information*

18. MKS develops, manufactures, and supplies instruments and components used to control and analyze gases in semiconductors and similar industrial manufacturing processes. The

Company offers products to manufacture flat panel displays, magnetic and optical storage devices and media, solar cells, fiber optic cables, and diamond thin films.<sup>2</sup>

19. As a condition of employment with MKS, Defendant requires that its employees entrust it with highly sensitive personal and medical information. In the ordinary course of employment with MKS, Plaintiff and Class Members were required to provide their Private Information to Defendant.

20. Because of the highly sensitive and personal nature of the information MKS acquires and stores with respect to its employees, MKS, upon information and belief, promises to, among other things: keep employees' Private Information private; comply with industry standards related to data security and the maintenance of its employees' Private Information; inform its employees of its legal duties relating to data security and comply with all federal and state laws protecting employees' Private Information; only use and release employees' Private Information for reasons that relate to the services it provides; not store former employees' Private Information for longer than is necessary to carry out its business operations; and provide adequate notice to its current and former employees if their Private Information is disclosed without authorization.

21. By obtaining, collecting, using, and deriving a benefit from its employees' Private Information, MKS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

22. Plaintiff and Class Members relied on MKS to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

---

<sup>2</sup> See <https://www.bloomberg.com/profile/company/MKSI:US#xj4y7vzkg> (last visited on April 27, 2023).

***B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members***

23. In a Form 8-k filed with the United States Securities and Exchange Commission on February 6, 2023, Defendant reported that it learned of unauthorized access to its computer systems on or around February 3, 2023.<sup>3</sup> According to the report, the Data Breach was the result of a ransomware attack, which ultimately “affected certain business systems, including production-related business systems...,” leading to the temporary “suspen[sion of] operations at certain of its facilities.”<sup>4</sup>

24. Through the Data Breach, the unauthorized cybercriminal(s) access and exfiltrated a cache of highly sensitive Private Information, including MKS’s current and former employees’ names, Social Security numbers, financial information, and PHI.

25. MKS had obligations created by contract, industry standards, and common law to keep Plaintiff’s and Class Members’ Private Information confidential and to protect it from unauthorized access and disclosure.

26. Plaintiff and Class Members provided their Private Information to MKS with the reasonable expectation and mutual understanding that MKS would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

27. MKS’s data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

28. MKS knew or should have known that its electronic records would be targeted by cybercriminals, yet it failed to take the necessary precautions to protect Plaintiff’s and Class Members’ Private Information from being compromised.

---

<sup>3</sup> See <https://investor.mks.com/node/21421/html> (last visited on April 27, 2023).

<sup>4</sup> *Id.*

**C. MKS Failed to Comply with FTC Guidelines**

29. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,* *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

30. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

31. The FTC further recommends that companies not maintain personally identifiable information (“PII”) longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

32. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

33. As evidenced by the Data Breach, MKS failed to properly implement basic data security practices. MKS's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information evidences its negligent failure to comply with the standards set forth by Section 5 of the FTCA.

34. MKS was at all times fully aware of its obligation to protect the Private Information of its current and former employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

#### **D. MKS Failed to Comply with HIPAA**

35. Title II of the Health Insurance Portability and Accountability Act ("HIPAA") contains what are known as the Administration Simplification provisions. *See 42 U.S.C. §§ 1301, et seq.* These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

36. MKS's Data Breach resulted from a combination of insufficiencies that indicate MKS failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from MKS's Data Breach that MKS either failed to implement, or

inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

37. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

38. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

39. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

40. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

41. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

42. Based upon Defendant's Notice to Plaintiff and Class Members, MKS reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

43. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

44. Because MKS provided notice, it reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not

permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

45. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

46. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

47. Because MKS provided notice, it reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

48. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

49. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

50. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

51. In addition, MKS's Data Breach could have been prevented if MKS had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its employees.

52. MKS's security failures also include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information MKS creates, receives, maintains, and/or transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

53. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required MKS to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach*” (emphasis added).

54. Because MKS has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure MKS's approach to information security is adequate and appropriate going forward. MKS still maintains the PHI and other highly sensitive PII of its current and former employees, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

#### ***E. MKS Failed to Comply with Industry Standards***

55. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect from current and former employees and maintain.

56. Some industry best practices that should be implemented by businesses like MKS include, but are not limited to, educating all employees, implementing strong password requirements, implementing multilayer security including firewalls, implementing anti-virus and anti-malware software, encrypting highly sensitive data, implementing multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow at least some, or perhaps all of, these industry best practices.

57. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

58. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

59. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

***F. MKS Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information***

60. In addition to its obligations under federal and state laws, MKS owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. MKS owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of its current and former employees.

61. MKS breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. MKS's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect current and former employees' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to fully comply with FTC and HIPAA guidelines for cybersecurity in violation of the FTCA and HIPAA;
- e. Failing to adhere to industry standards for cybersecurity as discussed above; and
- f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

62. MKS negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information and exfiltrate such Private Information.

63. Had MKS remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

64. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

***G. MKS Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft***

65. The FTC hosted a workshop to discuss "informational injuries," which are injuries that current and former employees like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.<sup>5</sup> Exposure of highly sensitive personal information that individuals to keep private may cause harm to them, such as the ability to obtain or keep employment. Individuals' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

66. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

---

<sup>5</sup> *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), available at [https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational\\_injury\\_workshop\\_staff\\_report\\_-oct\\_2018\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-oct_2018_0.pdf) (last visited on April 27, 2023).

67. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

68. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

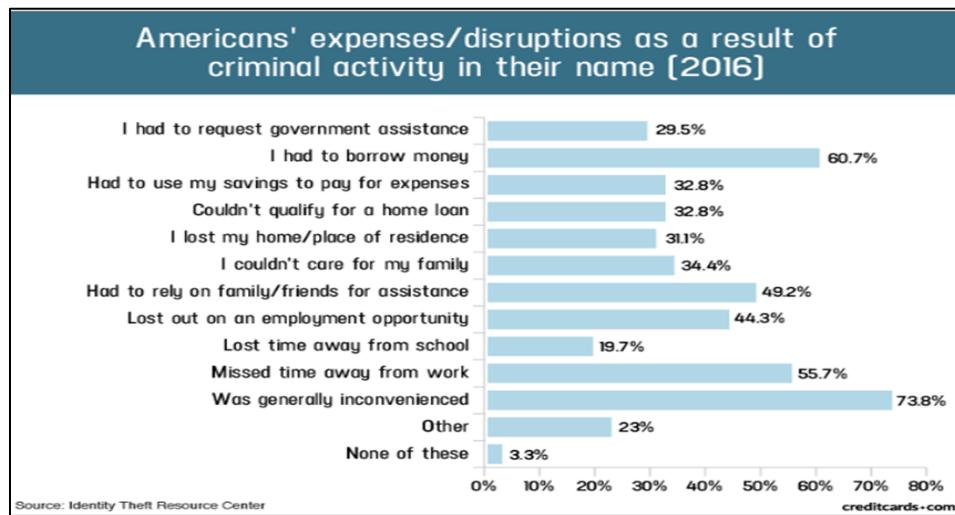
69. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

70. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.<sup>6</sup> However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

71. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

72. A study by the Identity Theft Resource Center<sup>7</sup> shows the multitude of harms caused by fraudulent use of PII:



<sup>6</sup> See *IdentityTheft.gov*, Federal Trade Commission, available at <https://www.identitytheft.gov/Steps> (last visited April 24, 2023).

<sup>7</sup> Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited April 27, 2023).

73. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.<sup>8</sup>

74. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

75. While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much as \$363 according to the Infosec Institute.<sup>9</sup>

76. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

77. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."<sup>10</sup>

---

<sup>8</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited on April 27, 2023).

<sup>9</sup> Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at: <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited on April 27, 2023).

<sup>10</sup> Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, available at: <https://kffhealthnews.org/news/rise-of-identity-theft/> (last visited on April 27, 2023).

78. Here, not only was sensitive PII compromised, but sensitive PHI as well. The value of such highly sensitive information is axiomatic. The value of “big data” in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that PII and PHI have considerable market value.

79. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII, PHI, and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:<sup>11</sup>

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

80. PII and PHI are valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black market” for years.

81. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future and have no choice but to vigilantly monitor their accounts and purchase credit monitoring and identity theft protection for many years to come.

#### ***H. Plaintiff's and Class Members' Damages***

##### *Plaintiff Sharma's Experience*

---

<sup>11</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html> (last visited April 25, 2023).

82. Plaintiff Sharma began his employment with MKS in March 2022 and worked for MKS until July 2022, though his Private Information inexplicably remained in MKS's systems after his employment ended and likely remains in MKS's possession and control.

83. In or around late February of 2023, Plaintiff Sharma received a letter entitled "Notice of Data Breach" which told him that his PII and PHI had been accessed and "may have been exfiltrated" during the Data Breach. The notice letter informed him that the Private Information stolen included his name, contact information, address, government ID numbers (including Social Security Number), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs (where MKS is required by law to collect), education, employment history, date of birth, gender, sexual orientation, bank account information, payment card information, information about compensation and equity, information about job position and time/hours worked, information about disabilities, health and medical conditions, employer union, health insurance information, basic information regarding partners, children and emergency contacts (such as name, age, and contact details), if applicable.

84. The notice letter offered Plaintiff Sharma only two (2) years of credit monitoring services. Two (2) years of credit monitoring is not sufficient given that Plaintiff Sharma will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

85. Plaintiff Sharma suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

86. Plaintiff Sharma would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices

to safeguard its employees' personal and health information from theft, and that those systems were subject to a data breach.

87. Plaintiff Sharma suffered actual injury in the form of having his PII and PHI compromised and stolen as a result of the Data Breach.

88. Plaintiff Sharma suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Sharma entrusted to Defendant for the purpose of receiving employment from Defendant and which was compromised in, and as a result of, the Data Breach.

89. Plaintiff Sharma suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

90. Plaintiff Sharma has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

91. As a result of the Data Breach, Plaintiff Sharma made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Sharma has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

92. As a result of the Data Breach, Plaintiff Sharma has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff Sharma is very concerned about this

increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

93. Plaintiff Sharma also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII and PHI, a form of property that Defendant obtained from Plaintiff Sharma; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

94. As a result of the Data Breach, Plaintiff Sharma anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

95. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

96. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive employment with Defendant.

97. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

98. As a direct and proximate result of MKS's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

99. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. Plaintiffs and Class Members will also eventually be forced to incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

102. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

103. Plaintiffs and Class Members also lost the benefit of the bargain they made with MKS. Plaintiffs and Class Members turned over valuable personal information to MKS that was intended to be accompanied by adequate data security but was not. Indeed, part of the value in the Private Information turned over by Plaintiffs and Class Members to MKS was intended to be used by MKS to fund adequate security of MKS's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

104. Additionally, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>12</sup> In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.<sup>13</sup> Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.<sup>14</sup>

105. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in both economic and noneconomic harm as alleged herein. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

106. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of MKS, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive

---

<sup>12</sup> See Data Coup, <https://datacoup.com/>.

<sup>13</sup> *What is digi.me?*, DIGI.ME, <https://digi.me/what-is-digime/> (last visited Jan. 16, 2023).

<sup>14</sup> *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited Jan. 16, 2023).

personal and health information of its current and former employees is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

107. As a direct and proximate result of MKS's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and cognizable harms, including imminent and substantial future risk of harm in the forms set forth herein.

#### **IV. CLASS ACTION ALLEGATIONS**

108. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

109. Specifically, Plaintiff proposes the following Nationwide Class and Utah Subclass (collectively referred to herein as the "Class"), subject to amendment as appropriate:

##### **Nationwide Class**

**All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.**

##### **Utah Subclass**

**All individuals residing in the state of Utah who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach**

110. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

111. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

112. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

113. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of at least 100 current and former employees of MKS whose data was compromised in the Data Breach and likely numbers in the tens of thousands. The identities of Class Members are ascertainable through MKS's records, Class Members' records, publication notice, self-identification, and other means.

114. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether MKS engaged in the conduct alleged herein;
- b. When MKS learned of the Data Breach;
- c. Whether MKS's response to the Data Breach was adequate;
- d. Whether MKS unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;
- e. Whether MKS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- f. Whether MKS's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- g. Whether MKS's data security systems prior to and during the Data Breach were consistent with industry standards;

- h. Whether MKS owed a duty to Class Members to safeguard their Private Information;
- i. Whether MKS breached its duty to Class Members to safeguard their Private Information;
- j. Whether hackers exfiltrated Class Members' Private Information via the Data Breach;
- k. Whether MKS had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- l. Whether MKS breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- m. Whether MKS knew or should have known that its data security systems and monitoring processes were deficient;
- n. What damages Plaintiff and Class Members suffered as a result of MKS's misconduct;
- o. Whether MKS's conduct was negligent;
- p. Whether MKS was unjustly enriched;
- q. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

115. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

116. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

117. Predominance. MKS has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from MKS's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for MKS. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

119. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). MKS has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

120. Finally, all members of the proposed Class are readily ascertainable. MKS has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by MKS.

**CLAIMS FOR RELIEF**

**COUNT I  
NEGLIGENCE  
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

121. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

122. MKS knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

123. MKS knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. MKS was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

124. MKS owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. MKS's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect current and former employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA and applicable industry standards;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To precisely disclose the type(s) of information compromised.

125. MKS's duty to employ reasonable data security measures to safeguard the Private Information in its possession arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

126. MKS's duty also arose under HIPAA, as set forth, *supra*, and because Defendant was also bound by industry standards to protect its current and former employees' confidential Private Information.

127. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and MKS owed them a duty of care not to subject them to an unreasonable risk of harm.

128. MKS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within MKS's possession.

129. MKS, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

130. MKS breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to comply with the FTCA and applicable industry standards;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

131. MKS had a special relationship with its current and former employees, including Plaintiff and Class Members.

132. Plaintiff's and Class Members' willingness to entrust MKS with their Private Information was predicated on the understanding that MKS would take adequate security precautions. Moreover, only MKS had the ability to protect its systems (and the Private Information stored thereon) from attack.

133. MKS's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated, as alleged herein and admitted by Defendant in its Notice to Plaintiff and Class Members.

134. MKS's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

135. As a result of MKS's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of criminal third parties, has been and will continue to be used for fraudulent purposes.

136. MKS also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information.

137. As a direct and proximate result of MKS's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

138. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

139. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

140. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring MKS to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

**COUNT II**  
**INVASION OF PRIVACY**  
**(ON BEHALF OF PLAINTIFF AND THE UTAH SUBCLASS)**

141. Plaintiff restates and realleges allegations stated from paragraphs 1-120 as if fully set forth herein.

142. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is highly sensitive, confidential information that is also protected from disclosure by applicable laws and industry standards, as set forth above.

143. Plaintiff's and Class Members' Private Information was contained, stored, and managed electronically in Defendant's records, computers, and databases and was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities were only shared with Defendant for the limited purpose of obtaining employment.

144. Additionally, Plaintiff's and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

145. Defendant's disclosure of Plaintiff's and Utah Subclass Members' Private Information to unauthorized third parties by allowing such parties to gain access to its network

resulted from Defendant's failure to adequately secure and safeguard Plaintiff's and Class Members' Private Information. Such failure was the direct and proximate cause of unauthorized intrusions into Plaintiff's and Utah Subclass Members' places of solitude and seclusion that are highly offensive to a reasonable person. Such disclosures also constitute unreasonable publicity given to Plaintiff's and Utah Subclass Members' lives.

146. Such exploitation of Plaintiff's and Class Members' Private Information was done for Defendant's business purposes.

147. MKS's unauthorized disclosure of Plaintiff's and Class Members' Private Information to criminal third parties permitted the electronic intrusion into private quarters where Plaintiff's and Class Members' Private Information was stored.

148. Plaintiff and Class Members have been damaged by MKS's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

**COUNT III**  
**BREACH OF IMPLIED CONTRACT**  
**(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

149. Plaintiff restates and realleges allegations stated from paragraphs 1-120 as if fully set forth herein.

150. MKS provided employment to Plaintiff and Class Members. In exchange for employment, Plaintiff and Class Members provided their valuable Private Information to MKS which, upon information and belief, MKS used to conduct and profit from its business.

151. Defendant, as employer, held the Private Information on behalf of Plaintiff and Class Members. Holding Plaintiff and Class Members' Private Information was part of Defendant's regular business practices, as agreed by the parties. When Plaintiff and Class

Members joined Defendant's employment, they agreed to turn over their valuable Private Information for storage within Defendant's network.

152. Plaintiff and Class Members entered implied contracts with Defendant in which Defendant agreed to safeguard and protect such Private Information and to timely detect any breaches of their Private Information. Plaintiff and Class Members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

153. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

154. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

155. Defendant breached these implied promises it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to notify Plaintiff and Class Members thereof within a reasonable time.

156. Plaintiff and Class Members would not have entrusted their Private Information to MKS in the absence of such an implied contract.

157. Had MKS disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices in place to secure such sensitive data, Plaintiff and Class Members would not have provided their Private Information to MKS.

158. MKS recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

159. MKS violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

160. Plaintiff and Class Members have been damaged by MKS's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

161. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class Members.

**COUNT IV**  
**UNJUST ENRICHMENT**  
**(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

162. Plaintiff restates and realleges allegations stated from paragraphs 1-120 as if fully set forth herein.

163. This Count is pleaded in the alternative to Count III above.

164. Plaintiff and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiff and Class Members should have been entitled to have Defendant protect

their Private Information with adequate data security, especially in light of their employer-employee relationship.

165. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff and Class Members' Private Information for business purposes.

166. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

167. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

168. If Plaintiff and Class Members knew that Defendant would not secure their Private Information using adequate security, they would have made alternative employment choices that excluded Defendant.

169. Plaintiff and Class Members have no adequate remedy at law.

170. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

171. As a direct and proximate result of MKS's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort

expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in MKS's possession and is subject to further unauthorized disclosures so long as MKS fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from MKS and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by MKS from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

173. Plaintiff and Class Members may not have an adequate remedy at law against MKS, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT V**  
**BREACH OF FIDUCIARY DUTY**  
**(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

174. Plaintiff restates and realleges allegations stated from paragraphs 1-120 as if fully set forth herein.

175. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by MKS and which

was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach. MKS, in taking possession of this highly sensitive information, formed a special relationship with its current and former employees, including Plaintiff and the Class.

176. Plaintiff and Class Members put their trust and confidence in MKS' judgment, honesty, and integrity in protecting their Private Information and the various accounts that could be accessed through use (or misuse) of that Private Information.

177. MKS knew that Plaintiff and Class Members were relying on MKS, and accepted this trust and confidence when it accepted possession of Plaintiff's and Class Members' Private Information.

178. As a result of that special relationship, MKS was provided with and stored private and valuable information belonging to Plaintiff and the Class, which MKS was required by law and industry standards to maintain in confidence.

179. In light of the special relationship between MKS and Plaintiff and Class Members, whereby MKS became a guardian of Plaintiff's and Class Members' Private Information, MKS undertook a fiduciary duty to act primarily for the benefit of its employees, including Plaintiff and Class Members, for the safeguarding of their Private Information.

180. MKS had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiff's and Class members' Private Information and to maintain the confidentiality thereof.

181. MKS owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

182. Plaintiff and Class Members have a privacy interest in their personal and proprietary matters and MKS had a duty not to disclose or allow unauthorized access to such confidential information.

183. Plaintiff's and Class Members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class Members did not consent to nor authorize MKS to release or disclose their PII to unknown criminal actors.

184. MKS breached its fiduciary duty to Plaintiff and Class Members when Plaintiff's and Class Members' Private Information was disclosed to unknown criminal hackers by way of MKS' own acts and omissions, as alleged herein.

185. MKS knowingly breached its fiduciary duties by failing to safeguard Plaintiff's and Class Members' PII, including by, among other things:

- a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of the Private Information;
- b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;
- c. failing to design and implement information safeguards to control these risks;
- d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

- f. failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class Members thereof;
- g. storing PII and PHI in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and
- h. making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' Private Information to a criminal third party.

186. But for MKS's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized criminal third parties with the intent to maliciously misuse it in the foreseeable future.

187. As a direct and proximate result of MKS's breach of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the MKS Data Breach—including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with law enforcement; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to MKS with the

mutual understanding that MKS would safeguard it against theft and not allow its access and misuse by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in MKS's possession and is subject to further breaches so long as MKS fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their Private Information.

188. MKS breached its fiduciary duty to Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for MKS to retain the benefits it has received at Plaintiff's and Class Members' expense.

189. Plaintiff and Class Members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and the Nationwide Class and Utah Subclass described above, seeks the following relief:

- a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and Utah Subclass requested herein;
- b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein, including but not limited to, an Order:

- 1) to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members; and
- 2) to comply with Defendant's explicit or implicit contractual obligations and duties of care through the implementation and ongoing observance of reasonable security measures, including, but not limited to:
  - i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on MKS's systems on a periodic basis, and ordering MKS to promptly correct any problems or issues detected by such third-party security auditors;
  - ii. engaging third-party security auditors and internal personnel to run automated security monitoring;
  - iii. auditing, testing, and training its security personnel regarding any new or modified procedures;
  - iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of MKS's systems;
  - v. conducting regular database scanning and security checks;
  - vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

- vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations;
- viii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and
- ix. meaningfully educating all Class Members about the threats they face with regard to the security of their Private Information, as well as the steps MKS's affected individuals should take to protect themselves.

- d. An order instructing MKS to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;
- e. An order requiring MKS to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all triable issues.

DATED: July 21, 2023

Respectfully submitted,

*/s/ Christina Xenides*

---

Christina Xenides  
Mason Barney (*pro hac vice* to be filed)  
Tyler Bean (*pro hac vice* to be filed)  
**SIRI & GLIMSTAD LLP**  
745 Fifth Avenue, Suite 500  
New York, New York 10151  
Tel: (212) 532-1091  
E: cxenides@sirillp.com  
E: mbarney@sirillp.com  
E: tbean@sirillp.com